REMARKS

By the present Amendment, Claims 4, 19, 27 and 28 have been amended and new Claims 29-30 have been added. Applicants have also amended the Specification on Page 10 to delete the reference number "207". No new matter has been added. Claims 1, 5-6, 13 and 20-21 were previously cancelled and Claims 25 and 26 were not entered. Thus, Claims 2-4, 7-12, 14-19, 22-24 and 27-30 are pending in this application.

A previous Office Action, dated January 20, 2007, stated that the IDS filed on December 20, 2004 was missing a copy of an International Search Report, issued in the corresponding PCT application filed the USPTO. Applicants attach herewith a copy of the International Search Report.

Applicants acknowledge the identification that Claims 4 and 19 may be allowable if amended into independent form including all of the limitations of the base claim and any intervening claims. However, Applicants wish to pursue the independent claims for the reasons cited below.

The Examiner has rejected Claims 7-8, 10-12, 16-18, 22, 23, 27 and 28 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 7,139,723 (Conkwright, et al., hereinafter "Conkwright") in view of U.S. Patent No. 6,272,152 (Levin, et al., hereinafter "Levin"). In particular, the Examiner asserts:

> As per claims 27 and 28, Conkwright et al. discloses a method and system for obscuring the identity of the course of a message while allowing the content of the message, and subsequent messages, issued from that source to be analyzed by a data analysis entity, and wherein the source is coupled to a cable television system operated by a system operator for receiving television programming content therefrom, comprising the steps of: forming the content of a message issued from the source to form a first message, said first message containing source identification indicia and wherein the

system operator knows the identity of the source of the said first message, said first message being transmitted upstream to a remote device on the cable television system (see column 4 line 58 through column 5 line 9); receiving said first message by said remote device (see column 10 lines 55-65); substituting said source identification indicia with anonymous identification indicia, wherein said anonymous identification indicia cannot be traced back to the source by the data analysis entity (see column 4 line 58 through column 5 line 17 and column 11 lines 5-17) and encrypting said first message along with said anonymous identification indicia into a second message and transmitting said second message to a location to be analyzed (see column 11 lines 5-39).

Conkwright fails to disclose encrypting and decrypting the first message.

However, Levin, et al. teaches obscuring the content of a message from a system operator by encrypting content of a message issued from the source to form a first message, said first message containing source identification indicia and wherein the system operator knows the identity of the source of said first message, said first message being transmitted upstream to a remote device on the cable television system (see column 23, lines 1-15); decrypting said first message into a first decrypted message upon receipt of said first message by said remote device (see column 4 line 61 through column 5 line 5 where the source address identifies the source).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to encrypt the first message of Conkwright.

Motivation, as recognized by one of ordinary skill in the art, to do so would have been to protect the privacy of the content.

Applicants respectfully disagree for the following reasons.

I. Conkwright does not "substitute" Source Identification with an AID in a Transmitted Message

Claim 27 recites "substituting said source identification indicia with anonymous identification indicia." Conkwright and Levin, whether taken alone or in combination, fail to teach or suggest this limitation.

The Conkwright system transmits viewer behavior data (e.g., channel changes, volume changes, muting, etc.)[1] from set top boxes (STBs)1100-1102, as most clearly shown in Fig. 11,

[1] Conkwright, col. 4, lines 15-22;

to a Head-end Bunker, either continuously or in batch[2]. This data[3] is then collected into tuner data 1105 (or 120 as shown in Fig. 1) which also resides in the Head-End Bunker[4]. It is in the Head-end Bunker, and more specifically, the UNIX-based server 1106 that allows collection of the viewer behavior data (also referred to as "STB data"). At that point, STB data is identified by zip code, area code and prefix, or other geographic identifier associated with the region of the STBs, based on pre-established correlations[5]. Thus, all of this tuner data 120, along with airings data 110, are then sent to a data center 130 (Fig. 1; Fig. 11) for analysis[6].

The upshot of this is that Conkwright does not teach or suggest encrypting, or in any manner, concealing the identity of the STB data during this transmission to the Head-end Bunker. Furthermore, once the data is transmitted to the Head-end Bunker, and the server 1106 forms the viewer behavior data, *there are no second, individual STB messages* requiring the introduction, let alone the substitution, of pseudo-identification indicia therein for re-transmission. As a result, Conkwright not only fails to teach or suggest encrypting the first message, but he fails to teach or suggest "*substituting," for example, the set top box identification data in a message issued by the set top box with anonymous identification data (AID) into a second message*, as now specified in Claim 27 and similarly now specified in Claim 28. Thus, for all of these reasons, Claims 27 and 28 are patentable over the art of record and Applicants respectfully request the withdrawal of the §103(a) rejection.

---

[2] Conkwright, col. 13, lines 14-19;
[3] In a preferred embodiment, individual-specific information, such as name, family size, business type, address, etc. is not even collected except for zip code, area code and prefix, or other geographic identifier. Conkwright, col. 13, lines 28-36;
[4] Conkwright, col. 9, lines 6-14;
[5] Conkwright, col. 11, lines 10-17;
[6] Conkwright, col. 9, lines 15-21;

II. Conkwright does not generate AID as the Source Message is Received

New Claim 29 recites the step of "generating anonymous identification data *upon receipt of said first message by said remote device.*" And, new Claim 30 recites "a generator adapted to generate anonymous identification indicia *upon receipt of said encrypted message.*" None of the cited references, whether taken alone or in combination, teaches or suggests these claim limitations.

According to Conkwright, the zip code, telephone number prefix, geographic code data, etc., that are used in the tuner data 1105 are *static*. In particular, Conkwright states that:

> ...To facilitate data analysis, ***a cable company can provide*** to the present invention a geographically associated code, such as, but not limited to, a zip code or telephone number prefix, that corresponds with each set-top box...(emphasis added, Conkwright, col. 4, lines 61-65).

And,

> ...Correlations between set top boxes and zip codes can be ***maintained*** in a cable television or other content provider's billing system; thus, access to such billing data may be preferred." (emphasis added, Conkwright, col. 11, lines 14-17).

This is in contrast to the invention recited in new Claims 29 and 30, where AID is generated "upon" receipt of the first message. For example, the specification discloses:

> ...Thus, each time the server receives the message EM1 from a particular source 1 and decrypts message EM1 into message DM1, the AID process extracts the same portion from the unique source ID number and then applies the mathematical hash to generate the same AID for each message subsequent that originates from that same source 1 and embed it in the message. (Present application, p. 12, lines 1-6).

To that end, new Claims 29-30 have been added and Applicants respectfully submit that they are patentable over the art of record.

III. One Skilled in the Art Would Not Have Combined Conkwright and Levin

Levin pertains to a 2-way cable transmission for effecting secure electronic transaction protocol, as well as a cable downstream/telephone upstream transmission secure electronic transaction, where a 2-way cable transmission is not available. The importance of secure communications between the source and destination, in both directions, is critical for *electronic sales*, especially where credit card/PIN data is being transferred[7]. To prevent the illicit interception and use of such critical data in such 2-way communication, encryption is used. However, in Conkwright, the content of the transmission between the STBs 1100-1102 and the Head-end Bunker is identification data and viewer behavior data[8], *not credit card or other personal financial data*. Furthermore, as stated previously, in the preferred embodiment of Conkwright, identification data (e.g., name, family size, business type, address, etc.) are not even collected except for zip code, area code and prefix, or other geographic identifier[9]. In addition, in Conkwright, the transmission of the identification data/viewer behavior data is one way: from the STBs to the Head-end Bunker, so the opportunities to illicitly intercept and use that data are greatly reduced as compared to the 2-way communication used in Levin. Once the identification data/viewer behavior data in Conkwright are delivered to the Head-end Bunker, that data are then combined with other viewer behavior data (tuner data 1105) along with zip code, telephone number prefix or other geographical data, all of which are then sent to the data center 130 for analysis. In view of the foregoing, Conkwright is thus not concerned with concealing the identity of such viewer behavior data in its transmission *from the STBs 1100-1102 to the Head-end*

[7] Levin, cols. 1-2;
[8] Conkwright, col. 4, lines 15-22;
[9] Conkwright, col. 13, lines 28-36;

Bunker. And in the preferred embodiment of Conkwright, it would appear redundant to implement encryption, especially where no *identification data* are included in the transmission from the STBs to the Head-end Bunker.

Thus, there is no reason to encrypt the STB data on its way to the Head-end Bunker in Conkwright, as proposed by the Office Action. The only reason to do some comes from using the present application as a template, which is not permitted under *In re Fitch*[10]. For all of these reasons, Applicants respectfully submit that one skilled in the art would not combine Conkwright with Levin and, as such, Applicants request that the §103(a) rejection of Claims 27-28 also be withdrawn.

With regard to dependent Claims 7, 8, 22 and 23 which relate to insertion of cable system source data into the first decrypted message, the Examiner rejects these claims under §103(a) citing Levin (col. 4, line 61 – col. 5, line 5) as teaching that the source and destination address define a network segment data. However, Levin does not teach *inserting* cable system source data (nor source and destination addresses, which the Examiner defines as "a network segment") into the *first decrypted* message; rather the source data, as well as the destination data, are inserted prior to *encryption*. (Levin, col. 4, lines 65-67). Thus, Applicants respectfully submit that for these additional reasons, and also because these claims ultimately depend from patentable Claims 27 and 28, respectfully, they are also patentable.

Claims 10 and 16 ultimately depend from Claims 27 and 28 respectively and are patentable for the same reasons.

---

[10] Moreover, the PTO may not "use the claimed invention as an instruction manual or 'template' to piece together the teachings of the prior art so that the claimed invention is rendered obvious." In re Fritch, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992).

Claims 11 and 12 depend from Claim 27 and Claims 17 and 18 ultimately depend from Claim 28 and are patentable for the reasons discussed previously with regard to amended Claims 27 and 28.

Claims 2, 3, 14 and 15 are directed to generating anonymous identification indicia using a hash algorithm, and which the Examiner rejects under §103(a) citing U.S. Patent Publication No. 2001/0036224 (Demello, et al, hereinafter "Demello") as teaching the same (viz., para. 0136 of Demello). Applicants respectfully submit that because these claims ultimately depend from Claims 27 and 28 respectfully, they are also patentable for the same reasons. Moreover, Conkwright does not *generate AID* but rather associates data with *pre-established* identifiers (e.g., zip code, area code and prefix or other geographic identifier)[11]. As such, this would *not give* any reason to one skilled in the art to leap to the use of pseudorandom numbers created by hash algorithms for generating identifiers, as specified in Claims 2, 3, 14 and 15. And as mentioned previously, in the preferred embodiment of Conkwright, since individual identity data would not even be collected[12] except for zip code, area code and prefix, etc. from the STBs, the need to generate AID is removed. Nor would the combination of Conkwright/Levin and Demello yield predictable results in view of their different operations. The Examiner is using the present invention as a template, in contravention to *In re Fitch,* to assert that one skilled art would combine the teachings of Demello with Conkwright and Levin to arrive at the inventions of Claims 2, 3, 14 and 15. Thus, Applicants respectfully request the withdrawal of the §103(a) rejection regarding Claims 2, 3, 14 and 15.

---

[11] Conkwright, col. 11, lines 10-17;
[12] Conkwright, col. 13, lines 28-36;

With regard to dependent Claims 9 and 24 which specify including cluster code data into the encrypted message, the Examiner rejects these claims under §103(a) citing U.S. Patent Publication No. 2002/0059632 (Link, et al.), as already disclosing this feature. Applicants respectfully submit that because these claims ultimately depend from amended Claims 27 and 28 respectfully, they are also patentable for the same reasons.

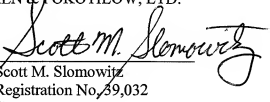
Thus, Applicants respectfully submit that Claims 2-4, 7-12, 14-19, 22-24 and 27-30 are in condition for allowance. Accordingly, prompt and favorable examination on the merits is respectfully requested.

Should the Examiner believe that anything further is desirable in order to place the application in even better condition for initial examination and allowance, the Examiner is invited to contact Applicant's undersigned attorney at the telephone number listed below.

Respectfully submitted,

CAESAR, RIVISE, BERNSTEIN,
COHEN & POKOTILOW, LTD.

March 23, 2009

By 

Scott M. Slomowitz
Registration No. 39,032
Customer No. 03000
(215) 567-2010
Attorneys for Applicants

Please charge or credit our Account No. 03-0075 as necessary to effect entry and/or ensure consideration of this submission.